26. Лаурент О. Борьба со спамом с помощью системы Honeypot: Часть 1 / О. Лаурент [Електр. ресурс] — Режим доступу: http://www.securitylab.ru/analytics/216335.php (04.09.2012).

27. Лаурент О. Борьба со спамом с помощью системы Honeypot: Часть 2 / О. Лаурент [Електр. ресурс] — Режим доступу: http://www.securitylab.ru/analytics/216343.php (04.09.2012).

28. Deal R. Router Firewall Security / R. Deal. — SF. : Cisco Press, 2004. — p. 912.

29. Honeywall project site [Електр. ресурс]: (Honeywall – Trac) // The Honeynet Project — Режим доступу: https://projects.honeynet.org/honey-wall (04.09.2012).

30. Argus and Infiniband [Електр. ресурс]: (ARGUS – Auditing Network Activity) // QoSient — Режим доступу: http://www.qosient.com/argus (04.09.2012).

31. What is p0f [Електр. ресурс]: (the new p0f) // lcamtuf.coredump.cx — Режим доступу: http://lcamtuf.coredump.cx/p0f.shtml (04.09.2012).

32. Balas E. Honeynet data analysis: A technique for correlating sebek and network data / E. Balas // Workshop on Information Assurance and Security US Military Academy, West Point, NY. — IEEE, 2004.

33. Хусни. Метод разработки средств автоматизации и проектирования сетей приманок : автореф. дис. на соискание науч. степени канд. техн. наук : спец. 05.13.19 «Методы и системы защиты информации, информационная безопасность» / Хусни. — СПб., 2010. — 17 с.

34. Тимошик Н.П. Вдосконалення принципів побудови та функціонування приманок в задачах захисту комп'ютерних систем та мереж : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.05 «Комп'ютерні системи та компоненти» / Н.П. Тимошик. — Львів, 2010. — 22 с.

Надійшла: 17.07.2012 р.

Рецензент: д.т.н., професор Корченко О.Г.

УДК 004.9:517.978.2

Грищук Р.В., Корченко О.Г.

МЕТОДОЛОГІЯ СИНТЕЗУ ТА АНАЛІЗУ ДИФЕРЕНЦІАЛЬНО-ІГРОВИХ МОДЕЛЕЙ ТА МЕТОДІВ МОДЕЛЮВАННЯ ПРОЦЕСІВ КІБЕРНАПАДУ НА ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ

У статті подано методологію синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу. Створена методологія з єдиних системних позицій дозволяє здійснювати синтез усіх диференціально-ігрових методів моделювання процесів кібернападу, які передбачають застосування комплексів відповідних моделей різного ступеню точності, від моделей оцінювання рівня захищеності – до моделей прогнозування розвитку динаміки процесу кібернападу. Застосування методології сприяє процесу інтеграції прогресивних систем інформаційної безпеки в новостворювані ІТ- технології, що, поряд з вирішенням основних завдань за призначенням, вирішують завдання інформаційної безпеки та є стійкими до прогнозованого класу кібератак і параметрів, які їх характеризують. Результати методології відображаються як у кількісній, так і якісній формі, що не суперечить основним положенням теорії складних систем.

Ключові слова: методологія синтезу та аналізу, диференціально-ігрові моделі та методи моделювання, інформаційний ресурс, процес кібернападу, рівень захищеності, кібератака, стратегія кіберзахисту, стратегія кібернападу.

Постановка проблеми. Стрімкий розвиток науково-технічного прогресу на початку XXI сторіччя в галузі інформаційних технологій (ІТ- технологій) пов'язаний з повсюдним впровадженням їх у всі сфери діяльності сучасного суспільства будь-якої розвиненої держави світу. Високі темпи інформатизації українського суспільства та державних інститутів сприяють подальшому зростанню ролі й місця кіберпростору в питаннях забезпечення національної безпеки в інформаційній сфері. Кіберпростір на сьогодні виступає системоутворюючим чинником, безпека якого не в останню чергу визначає рівень інформаційної безпеки (ІБ) держави. Масова доступність ІТ- технологій відкриває широкі можливості щодо здійснення несанкціонованого доступу (НСД) до державних інформаційних ресурсів (ІР) як неавторизованим користувачам, так і злочинним угрупованням, чим створює передумови для виникнення загроз безпеці інформації у національному сегменті кіберпростору в інформаційній сфері [1]. Протидія таким загрозам є принциповим аспектом укріплення стратегічної стабільності держави та її ІБ [2]. Безпрецедентний у світовій практиці за своїми аналогами й наслідками для органів державної влади інцидент з ІБ, пов'язаний з масованим кібернападом (КБн) на державні ІР, що відбувся в лютому 2012 року в національному сегменті кіберпростору, спонукає до

перегляду діючих концепцій побудови систем ІБ (СІБ) та стратегій їх ефективного застосування.

Аналіз останніх досліджень і публікацій [1–5] дозволив встановити один з пріоритетних напрямків підвищення рівня захищеності (РЗ) ІР зокрема, та подальшої стабілізації ІБ держави в цілому. Він полягає в якісно новому вирішенні проблеми ІБ держави шляхом створення сучасних методів та засобів захисту інформації (ЗІ) від КБн, що реалізують НСД до ІР інформаційно-телекомунікаційних систем та технічних об'єктів їх інфраструктури. Так, вагомі наукові результати при вирішенні проблеми ІБ держави та розкритті окремих її складових одержано в наукових працях [1–3, 6–11] та ін., але незважаючи на це проблема залишається актуальною не тільки для України, а й для усієї світової спільноти.

Виходячи з єдиних системних позицій [12, 13] та потреби реалізації комплексного підходу до побудови прогресивних СІБ на сучасному етапі розвитку науки і техніки існує об'єктивне протиріччя між високими вимогами, що висуваються до забезпечення захищеності ІР в умовах інформаційного конфлікту (ІК) під час реалізації процесів КБн, та принциповою неможливістю їх виконання на базі сучасної практики ЗІ, яка ґрунтується на застарілих моделях і методах. Крім того, відсутність єдиного методологічного базису надалі загострює проблему ІБ. Таким чином, подальший розвиток математичного інструментарію для дослідження проблеми ІБ держави є актуальним науковим завданням, що потребує вирішення.

У зв'язку з цим, метою статті є розробка відповідної методології синтезу та аналізу моделей і методів моделювання процесів КБн, необхідної та достатньої для розв'язання низки практичних задач ЗІ.

Основні матеріали дослідження. Відомо [14], що в основу математичних моделей та методів моделювання процесів КБн покладено три базові підходи – теоретичний, емпіричний та теоретико-емпіричний. Вказані підходи ґрунтуються на методах таких теорій: підтримки та прийняття рішень, множин, графів, ігор, збурень, ймовірностей, мереж Петрі та напівмарковських процесів, а також методів матричного та економічного аналізу, нейронних мереж та ланцюгів Маркова, методів оптимізації, логіки та теорії трафіка. Групування визначеного математичного інструментарію дозволило встановити, що усі відомі моделі на базі вищевказаних методів можуть бути віднесені до трьох основних класів – статичних, стохастичних та динамічних. У [14] показано, що застосування відомих моделей дозволяє отримувати кількісні, якісні та кількісно-якісні оцінки РЗ ІР, але на практиці ці моделі обмежено придатні для оцінювання прогнозованого РЗ, оскільки його необґрунтоване завищення або заниження може призвести до значних фінансових витрат. При цьому переважна більшість моделей та методів призначені для моделювання процесів кіберзахисту (КБз). Тобто, проблема антагоністичної взаємодії суб'єктів ІК – гравців, розкривається лише частково, а тому створювані СІБ не в повній мірі є адекватними існуючим загрозам ІБ.

Таким чином, як зрозуміло з вищевикладеного, на основі існуючого методологічного апарату досить проблематично досягнути поставленої в статті мети.

Для повноти опису процесів КБн в сучасних умовах доцільно застосовувати принципово нову концепцію моделювання, яка ґрунтується на синтезі методів теорії диференціальних ігор (ДІ) [15] та диференціальних перетворень (ДП) [16]. За результатами патентного пошуку, критичного аналізу захищених дисертацій, монографій, НД та ДКР за визначеною в статті темою, доступних з відкритого друку, встановлено, що до сьогодні в галузі ІБ держави така концепція моделювання і, відповідно, математичні інструменти не використовувалися раніше, чим визначається науковий пріоритет дослідження.

Ефективність моделювання процесів КБн методами теорії ДІ та ДП обумовлена рядом обставин [14]:

– диференціально-ігрові моделі та методи моделювання відкривають можливості дослідження розвитку динаміки процесів КБн, враховують їх рандомізоване походження, а також адекватно відображають антагонізм інтересів суб'єктів ІК – гравців. Антагонізм, породжений протиріччям інтересів і цілей гравців, є джерелом ІК. ІК, як системне явище,

характеризується структурними, динамічними та теоретико-ігровими властивостями, нехтувати жодною з яких – неможливо. Застосування диференціально-ігрових моделей та методів моделювання сприятиме на практиці виробленню ефективних превентивних заходів, спрямованих на ЗІ;

– застосування операційного методу ДП академіка НАН України Г. Є. Пухова дозволяє розв'язувати складні диференціально-ігрові задачі в області зображень з відсутнім безперервним аргументом і зводити їх до більш простих, які легко розв'язуються відомими методами. На відміну від інших операційних методів, наприклад інтегральних перетворень Лапласа, Мелліна, Фур'є тощо, область моделювання ДП не обмежується лінійними рівняннями.

Перевагою ДП над іншими операційними методами є можливість проведення моделювання в аналітичному, цілочислово-аналітичному та цілочисловому вигляді за відсутності методичної похибки методу. Властивість адаптованості ДП до вибору форми моделювання підвищує ефективність методів синтезу та аналізу СІБ, а також процесів, що моделюються. Відсутність методичної похибки забезпечує достовірність методів та адекватність моделей реальним процесам. Можливість отримання аналітичних моделей з використанням методу ДП відкриває нові шляхи для впровадження в практику захисту широкого класу прогресивних СІБ.

Математичне моделювання прикладних задач ЗІ методами теорії ДІ ґрунтується на дотриманні таких чинників, які на вербальному рівні визначають сутність даної теорії: наявність системи диференціальних рівнянь (диференціального рівняння як частинний випадок), яка описує зміну в часі параметрів процесів, що моделюються; визначення допустимих керувань гравців у вигляді класу функцій, на які накладаються відповідні обмеження, що витікають із змісту задач ЗІ; встановлення цілей гравців у вигляді функціоналів, які визначені на розв'язках системи диференціальних рівнянь; інформація, що доступна гравцям на момент початку гри та в процесі її розвитку.

Зважаючи на поставлену мету дослідження, загальноприйнята термінологія ДІ [15] в статті інтерпретується так: суб'єкти ІК називаються гравцями КБн та КБз, правила поведінки гравців – стратегіями. Стратегії гравців вибираються в ігрових задачах з умови оптимізації деякого критерію – РЗ, який називається платою. Рішення диференціального рівняння називається траєкторією гри (партії) – моделлю процесу КБн. Під ціною гри – прогнозованим РЗ, розуміють плату, яка виражена через оптимальні стратегії розподілу ресурсів гравців. Основна задача диференціальних ігор полягає у визначенні ціни гри, оптимальних стратегій поведінки гравців та траєкторій, що відповідають оптимальним стратегіям.

Спираючись на відомий підхід до побудови методологій [13], в статті, на основі досліджень [18–47], пропонується методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів КБн. Вона містить шість етапів (рис.): 1) визначення множини станів СІБ; 2) вибір стратегій КБз; 3) оптимізація стратегій КБз та оцінювання РЗ; 4) прогнозування розвитку динаміки процесу КБн; 5) оптимізація ресурсів КБз та оцінювання РЗ; 6) оцінювання ефективності СІБ.

1. Визначення множини станів СІБ. На першому етапі, виходячи з того які характеристики безпеки ІР повинні бути забезпечені (конфіденційність, цілісність, доступність) та множини параметрів, що визначають інтенсивності реалізації кібератак (КБа) $\mu_i(t)$ ($i=\overline{1,n}$, де n – кількість КБа), відмов СІБ $\beta_i(t)$, знаходження вразливостей $\gamma_i(t)$ тощо, експертом з ІБ вирішується концептуальне завдання щодо визначення множини можливих станів $\{P_z(t)\}$, у яких може перебувати новостворювана СІБ ($P_z(t)$ – ймовірності перебування СІБ під впливом відповідних методів, $z=\overline{0,c}$, c – кількість станів СІБ). Наприклад, якщо $z=0$, то СІБ у момент часу t перебуває під впливом методів НСД, якщо $z=1$ – під впливом МЗІ тощо.

2. Вибір стратегій КБз. На основі сформованої множини можливих станів СІБ $\{P_z(t)\}$, класу КБа і параметрів, які її характеризують, обирається стратегія КБз: стратегія побудови СІБ реального часу (РЧ); стратегія ешелонованого захисту (СЕЗ); стратегія відведення гравця КБн на псевдосервіс (ПсС); стратегія відведення гравця КБн на псевдосервіс з подальшим втягуванням його в ІК (ПсС та ІК); стратегія КБз, що характеризується змінними потоками захисних дій (ЗП); стратегія розподіленого (Р) захисту.

Як результат, за обраною стратегією будується граф станів СІБ під час КБа при реалізації процесу КБн та формалізується модель ІК, яка у подальшому використовується як вихідна для моделювання процесу КБн [19–25, 37–42].

3. Оптимізація стратегій КБз та оцінювання РЗ. На третьому етапі, на основі методу диференціально-ігрового моделювання [18] здійснюються процедури оптимізації обраних на етапі 2 стратегій КБз $\lambda_{z\min}^{opt}(t)$ [19–23, 37–42] та оцінювання прогнозованого РЗ $I^*\left(\lambda_{z\min}^{opt}, \mu_{z\max}^{opt}\right)$. Кількісні оцінки поточного I та прогнозованого I^* РЗ знаходяться в інтервалі $I, I^* \in [0,1]$. Чим ближче оцінка наближається до 0, тим РЗ вищий.

Процедура оптимізації на третьому етапі реалізується у відповідному блоці, а в блоці оцінювання реалізується процедура оцінювання прогнозованого РЗ. Одержані дані з вказаних блоків є вихідними даними для наступного, четвертого етапу.

4. Прогнозування розвитку динаміки процесу КБн. На четвертому етапі віршується завдання прогнозування розвитку динаміки процесу КБн $P_0^{opt}(t)$ на основі комплексу однокритерійних диференціально-ігрових моделей (ОДІМ) $P_0^{NT}(t)$, $P_0^{G\,Lopt}{}_{P}(t)$ та $P_0^{opt}{}_{i}(t)$ [26–30]. Комплекс ОДІМ прогнозування розвитку динаміки процесів КБн ґрунтується на ряді як відомих, так і розроблених в [28] нових методах моделювання. З цією метою на блок аналізу, окрім оцінок $\lambda_{z\min}^{opt}(t)$ та I^*, надходять вимоги, що висуваються до похибки моделі 2^q (q – кількість дискрет, які враховуються для диференціальних спектрів (ДС) $P_0(k)$ при побудові відповідної моделі (k – цілочисловий аргумент, $k =: 0,1,2,...$)), її точності y^*, а також діапазону прогнозування $t \in [t_0, T]$ на якому вона працює із заданими характеристиками. Виходячи з висунутих вимог обирається один з трьох диференціально-ігрових методів моделювання: метод моделювання на основі нетейлорівських перетворень (НТ) – метод НТ [27]; метод гібридного (ГБ) моделювання – метод ГБ [28]; метод числово-аналітичного моделювання (ЧАМ) – метод ЧАМ [29]. Далі будується відповідна диференціально-ігрова модель прогнозування розвитку динаміки процесу КБн – НТ диференціально-ігрова модель $P_0^{NT}(t)$, ГБ P-L модель $P_0^{G\,Lopt}{}_{P}(t)$ або неперервна-дискретна (НД) диференціально-ігрова модель $P_0^{opt}{}_{i}(t)$. Згідно з [37] найвищу точність прогнозування мають моделі побудовані на основі методу гібридного P-L-моделювання [28].

5. Оптимізація ресурсів КБз та оцінювання РЗ. На цьому етапі вирішуються ряд задач. Основна задача – це задача оптимізації обмеженого ресурсу КБз $\lambda_{z\min}^{opt}(t)$ за умови відповідності поточного РЗ прогнозованому, який не гірше за ціну гри I_0^{VR}. Другорядна задача – задача підвищення достовірності одержуваних оцінок прогнозованого РЗ та адекватності відповідних багатокритерійних диференціально-ігрових моделей $P_0^{opt^{VR}}(t)$. Вказані задачі вирішуються шляхом введення експертом з ІБ додаткових частинних критеріїв $I_j = \hat{O}_j[\lambda_i(t), \mu_i(t), T, P_0(t)]$, що характеризують той чи інший аспект функціонування СІБ ($\hat{O}_j$ – функції, що мають неперервні частинні похідні за $\lambda_i(t)$ та $\mu_i(t)$).

Частинні критерії I_j є компонентами r-мірного векторного критерію $I_0 = \overline{I_1, I_r}$, який обмежений допустимою областю $I_0 \in M$. Наприклад, додатковими частинним критеріями є ресурс (Р) гравця КБз I_2, Р гравця КБн I_3.

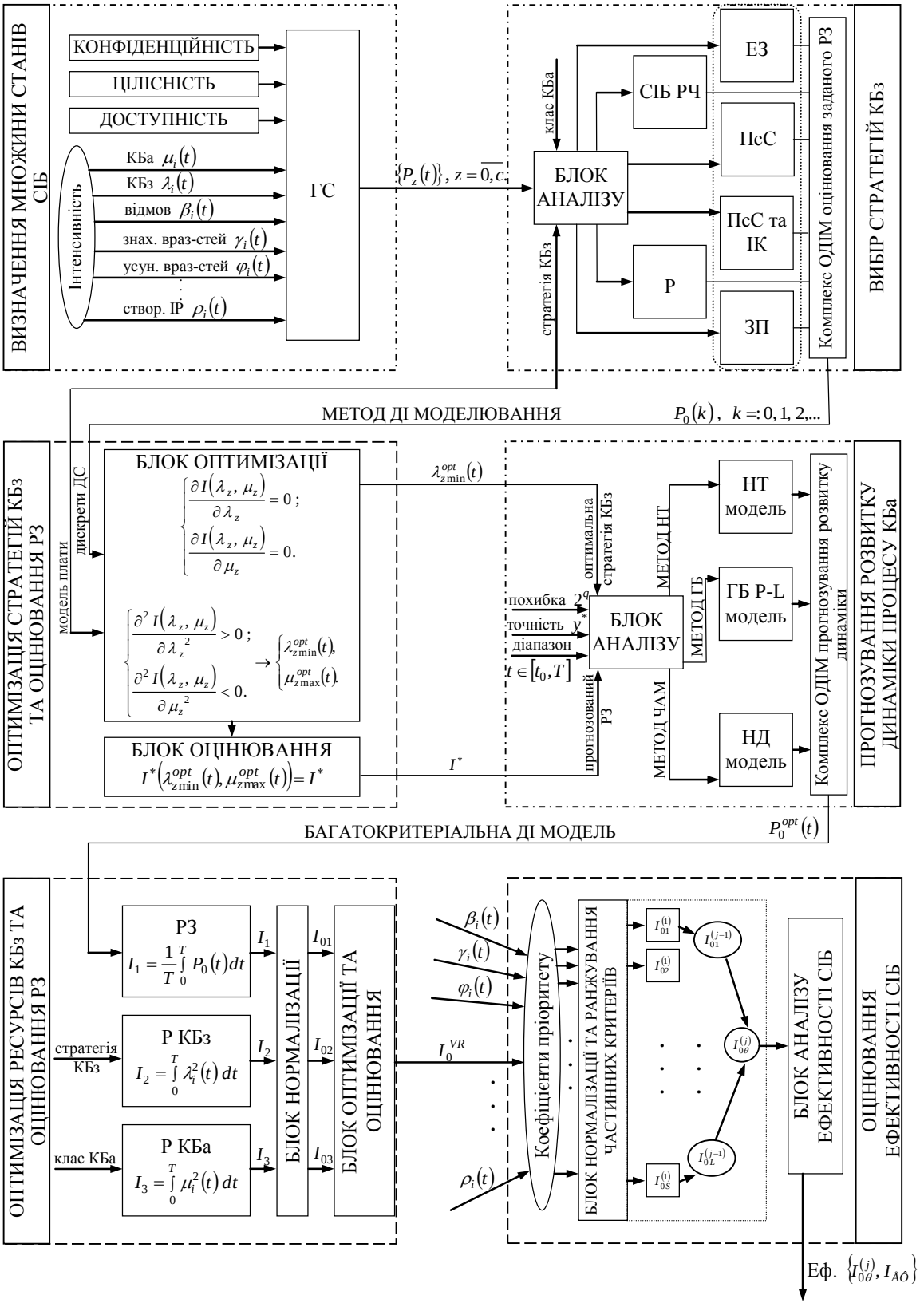

Рис. Схема методології синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу

Процедура багатокритеріального оцінювання реалізується із застосуванням відповідної багатокритерійної диференціально-ігрової моделі [31–33], яка грунтується на

методі диференціально-ігрового моделювання (етап 2) та нелінійній схемі компромісів. Так, усі частинні критерії I_j надходять на блок нормалізації, де реалізується процедура їх нормалізації шляхом зведення до безрозмірної величини I_{0j}. У блоці оптимізації та оцінювання здійснюється процедура регуляризації вихідної некоректної задачі моделювання процесів КБн за багатокритерійною диференціально-ігровою моделлю, забезпечується суттєве спрощення проблеми динамічної векторної оптимізації.

6. Оцінювання ефективності СІБ. Шостий етап є заключним. Він передбачає реалізацію диференціально-ігрової процедури оцінювання ефективності СІБ [35, 36, 41, 42, 47], яка проектується. Так, при проектуванні СІБ експерт вирішує завдання забезпечення вибору найефективнішої альтернативи $I_{0\theta}^{(j)*}$ з можливих, тобто $I_{0\theta}^{(j)*} \in \left\{I_{0\theta}^{(j)}\right\}$ (j – рівень ієрархії частинних критеріїв, θ- ї властивості, що оцінюється). Для множини властивостей, що оцінюються, розраховуються коефіцієнти пріоритету $\alpha_{S\theta}^{(j-1)} = f_{S\theta}\left[\sum_{S=1}^{L_\theta^{(j-1)}} f_{S\theta}\right]^{-1}$, $\theta \in \left[1, L^{(j)}\right]$, $j \in [2, m]$, де $\alpha_{S\theta}^{(j-1)}$ – S-а компонента вектора пріоритету критерію на $(j-1)$-у рівні ієрархії при розрахунках ефективності θ-ї властивості j-го рівня ($S \in \left[1, L^{(j-1)}\right]$, $L^{(j-1)}$ – кількість частинних критеріїв, за якими оцінюється ефективність СІБ на $(j-1)$-у рівні ієрархії); $f_{S\theta}$ – оцінка важливості S-ї властивості $(j-1)$-го рівня ієрархії для θ-ї властивості j-го рівня, визначена експертом з ІБ за шкалою балів. У блоці нормалізації та ранжування частинних критеріїв здійснюється процедура приведення усіх частинних критеріїв до однієї безрозмірної форми та ранжування їх у вигляді структурної схеми. У блоці аналізу, на основі диференціально-ігрового методу оцінювання ефективності СІБ [34], знаходяться кількісні та якісні оцінки ефективності системи $\left\{I_{0\theta}^{(j)*}, I_{\hat{A}\hat{O}}\right\}$ ($I_{\hat{A}\hat{O}}$ – базова терм-множина лінгвістичної змінної, яка визначається п’ятьма термами: $I_{\hat{A}\hat{O}} = \bigcup_{i=1}^{5} I_{\hat{A}\hat{O}} =$ {"абсолютно неефективна" (АН), "недостатньо ефективна" (НЕ), "ефективна" (Е), "достатньо ефективна" (ДЕ), "абсолютно ефективна" (АЕ)}). Застосування методу [34] забезпечує оцінювання ефективності СІБ на різних рівнях ієрархії, що сприяє розширенню діапазону його практичного застосування на процедури оцінювання ефективності комплексних СІБ, як діючих, так і перспективних.

На рис. штриховою лінією виділено порядок розв’язання оберненої задачі – задачі синтезу, яка полягає у знаходженні прогнозованого РЗ – I^* та оптимальних стратегій захисту $\lambda_{i\min}^{opt}(t)$ при найгірших, з точки зору захищеності ІР проявах кібератак гравцем кібернападу $\mu_{i\max}^{opt}(t)$; лінією в крапку виділено порядок розв’язання прямої задачі – задачі аналізу, яка полягає у знаходженні в аналітичному вигляді диференціально-ігрових моделей процесів КБн $P_0^{opt}(t)$. У результаті застосування методології формується звіт, у якому відображаються результати 1–6 етапів. Отримані результати можуть бути використані для формування додаткових наборів вхідних даних, які слід враховувати при проектуванні та створенні прогресивних СІБ. Особливістю методології є те, що кожен з визначених етапів може бути реалізований як окремо, так і в сукупності з іншими. Так, наприклад, розроблені на третьому та четвертому етапах моделі знайшли своє місце при удосконаленні математичного забезпечення систем виявлення атак на державні ІР та використані на практиці для побудови шаблону нормальної поведінки Web-сервера Apache 2.2.10 (Linux|SUSE) та шаблону атаки (для атаки, спрямованої на сканування портів; DoS-, DDoS-атак) [43–46].

Висновки. На основі запропонованої методології синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів КБн можливо будувати як програмні, так і програмно-апаратні СІБ, інтегровані до новостворюваних ІТ- технологій, що призначені для забезпечення в реальному масштабі часу прогнозованого РЗ ІР від кібератак прогнозованого класу. Застосування методології також забезпечує вибір найкращого варіанту побудови прогресивної СІБ, що ґрунтується на інтегральному показнику ефективності системи на базі розроблених моделей та методів моделювання. Створена на основі диференціально-ігрових моделей та методів методологія дозволяє оцінювати поточний та прогнозований РЗ, а також забезпечує прогнозування розвитку динаміки процесу КБн, протягом якого поточний рівень відповідатиме заданому, що сприятиме вибору превентивних стратегій КБз, адекватних умовам протікання ІК в СІБ.

ЛІТЕРАТУРА

1. Хорошко В. О. Информационная безопасность Украины. Основные проблемы и перспективы / В. О. Хорошко // Захист інформації. – 2008. – № 40 (спец. вип.). – С. 6–9.
2. Ленков С. В. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008. – 344 с.
3. Марущак А. І. Щодо поняття інформаційні ресурси держави / А. І. Марущак. – Інформаційна безпека людини, суспільства, держави. – 2009. – № 1(1). – С. 11–15.
4. Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями : монография / В. А. Голубев. – Запорожье : ЗИГМУ, 2003. – 336 с.
5. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / А. А. Малюк. – М. : Горячая линия – Телеком, 2004. – 280 с.
6. Андон П. І. Атаки на відмову в мережі Інтернет: опис проблеми та підходів до її вирішення / П. І. Андон, О. П. Ігнатенко. – К. : Ін-т ПС, 2008. – 52 с. – (Препринт / НАН України, Ін-т програмних систем).
7. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : "МК-Прес", 2005. – 432 с.
8. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К. : ООО "ТИД "ДС", 2004. – 992 с.
9. Кобозєва А. А. Аналіз стану й технології функціонування систем захисту інформації на основі теорії збурень : автореф. дис. на здобуття наук. ступеня док. тех. наук : спец. 05.13.21 "Системи захисту інформації" / А. А. Кобозєва. – К., 2008. – 39 с.
10. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новиков. За заг. ред. академіка НАН України М. З. Згуровського. – К. : Видавнича група BHV, 2009. – 608 с.
11. Голубенко О. Л. Політика інформаційної безпеки / О. Л. Голубенко, В. О. Хорошко, О. С. Петров та ін. – Луганськ : СНУ ім. В.Даля, 2009 – 376 с.
12. Корченко О. Г. Системи захисту інформації : монографія / О. Г. Корченко. – К. : НАУ, 2004. – 264 с.
13. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения : монография / А. Г. Корченко. – К. : "МК-Пресс", 2006. – 320 с.
14. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.
15. Айзекс Р. Дифференциальные игры : монография / Р. Айзекс. – М. : Мир, 1967. – 479 с.
16. Пухов Г. Е. Дифференциальные преобразования и математическое моделирование физических процессов : монография / Г. Е. Пухов. – К. : Наук. думка, 1986. – 160 с.
17. Грищук Р. В. Диференціально-ігрова модель кількісної оцінки захищеності технічних об'єктів / Р. В. Грищук // Захист інформації. – 2008. – № Спеціальний випуск (40). – С. 24–29.
18. Грищук Р. В. Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію / Р. В. Грищук // Інформаційна безпека. – 2009. – № 2 (2). – С. 128–132.
19. Грищук Р. В. Диференціально-ігрова розгалужена спектральна модель процесу нападу на інформацію / Р. В. Грищук // Вісник Житомирського державного технологічного університету. – 2009. – № І (48). – С. 152–159.
20. Грищук Р. В. Диференціально-тейлорівська модель перебування технічного об'єкта під впливом методів несанкціонованого доступу / Р. В. Грищук // Захист інформації. – 2009. – № 1 (42). – С. 19–27.
21. Грищук Р. В. Спектральна модель процесу нападу на інформацію / Р. В. Грищук // Захист інформації. – 2009. – № 2 (43). – С. 71–81.
22. Грищук Р. В. Р-моделювання процесів нападу на інформацію при нестаціонарній природі потоків захисних дій та інформаційних атак / Р. В. Грищук // Системи обробки інформації. – Х. : ХУПС ім. І. Кожедуба, 2009. – № 7 (79). – С. 98-101.
23. Грищук Р. В. Диференціально-ігрова модель системи захисту інформації при нестаціонарній природі потоків захисних дій та інформаційних атак / Р. В. Грищук // Інформаційна безпека. – 2010. – № 2 (4). – С. 23–29.

24. Грищук Р. В. Концепція побудови диференціально-ігрових гарантовано захищених розподілених систем захисту інформації / Р. В. Грищук // Сучасний захист інформації. – 2011. – № 1 (6). – С. 4–9.

25. Грищук Р. В. Диференціально-ігрова модель гарантовано захищеної розподіленої системи захисту інформації / Р. В. Грищук // Захист інформації. – 2011. – № 1 (50). – С. 20–28.

26. Грищук Р. В. GIGW гібридна P-L-модель процесу нападу на інформацію / Р. В. Грищук, В. О. Хорошко // Зб. наук. пр. СНУЯЕтаП. – Севастополь : СНУЯЕтаП. – 2009. – № 2 (30). – С. 153–160.

27. Грищук Р. В. Нетейлорівська модель процесу нападу на інформацію / Р. В. Грищук // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2009. – № 6 (136). – С. 60–64.

28. Грищук Р. В. Метод гібридного P-L-моделювання процесів нападу на інформацію / Р. В. Грищук // Зб. наук. пр. Військового інституту Київського національного університету імені Тараса Шевченка. – К. : ВІКНУ, 2009. – № 19. – С. 90–94.

29. Грищук Р. В. Неперервна дискретна диференціально-ігрова модель процесу нападу на інформацію / Р. В. Грищук // Вісник Житомирського державного технологічного університету. – 2009. – № IV (51). – С. 135–141.

30. Грищук Р. В. GIGW спектральна P-модель процесу нападу на інформацію / Р. В. Грищук // Зб. наук. пр. СНУЯЕтаП. – Севастополь : СНУЯЕтаП, 2010. – № 1 (33). – С. 188–195.

31. Грищук Р. В. Застосування багатокритеріальної моделі інтегральної оптимальності в задачах моделювання процесів нападу на інформацію P-перетвореннями / Р. В. Грищук // Захист інформації. – 2009. – № 3 (44). – С. 6–15.

32. Грищук Р. В. Багатокритеріальна модель процесу нападу на інформацію / Р. В. Грищук // Защита информации: сб. научн. тр. – К. : НАУ, – 2009. – № 16. – С. 290–295.

33. Грищук Р. В. Диференціально-ігрові моделі векторної оптимізації процесів нападу на інформацію / Р. В. Грищук // Інформаційна безпека. – 2010. – № 1 (3). – С. 79–85.

34. Грищук Р. В. Диференціально-ігровий метод оцінювання ефективності систем захисту інформації / Р. В. Грищук // Сучасний захист інформації. – 2012. – № 1 (10). – С. 40–44.

35. Грищук Р. В. Диференціально-ігровий метод аналізу надійності систем захисту інформації, на основі їх спектральних P-моделей / Р. В. Грищук // Захист інформації. – 2010. – № 4 (49) – С. 66–73.

36. Грищук Р. В. Ієрархічна диференціально-ігрова модель в задачах оцінювання ефективності систем захисту інформації / Р. В. Грищук // Інформатика та математичні методи в моделюванні. – 2011. – № 2. – С. 107–115.

37. Грищук Р. В. Верифікація і дослідження спектральних P- та гібридних P-L-моделей процесу нападу на інформацію / Р. В. Грищук // Вісник Житомирського державного технологічного університету. – 2009. – № II (49). – С. 69–76.

38. Грищук Р. В. Методика оцінювання гарантованого рівня захищеності технічних об'єктів / Р. В. Грищук, О. О. Хмара // Системи озброєння і військова техніка. – 2009. – 2 (18). – С. 74–78.

39. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах / Р. В. Грищук // Сучасна спеціальна техніка. – 2011. – № 1 (24). – С. 61–66.

40. Грищук Р. В. Синтез оптимальної поведінки в системі захист-атака / Р. В. Грищук, В. О. Хорошко // Проблеми створення, випробування та експлуатації складних інформаційних систем : зб. наук. пр. – Житомир : ЖВІ НАУ, 2011. – № 5. – С. 60–66.

41. Грищук Р. В. Постановка задачі розробки методики скорочення розмірності потоку вхідних даних для мережних систем виявлення атак / Р. В. Грищук, В. М. Мамарєв // Інформаційна безпека. – 2011. – № 1 (5). – С. 74–78.

42. Грищук Р. В. Метод оцінювання інформативності параметрів потоку вхідних даних для мережевих систем виявлення атак / Р. В. Грищук, В. М. Мамарєв // Системи обробки інформації. – Х. : ХУПС ім. І. Кожедуба, 2012. – № 4 (102). – С. 103–107.

43. Грищук Р. В. Диференціально-ігрова модель шаблону нормальної поведінки Web-серверу [Електронний ресурс] / Р. В. Грищук // Проблеми телекомунікацій. – 2010. – № 2 (2). – С. 96–106. – Режим доступу до журн. : http://pt.journal.kh.ua/2010/2/2/102_gryschuk_web.pdf.

44. Грищук Р. В. Диференціально-ігрова модель шаблону атаки на Web-сервер / Р. В. Грищук // Зб. наук. пр. Військового інституту Київського національного університету імені Тараса Шевченка. – К. : ВІКНУ, 2010. – № 27. – С. 104–112.

45. Грищук Р. В. Використання диференціальних ігор для оптимізації управління в системах захисту інформації / Р. В. Грищук, В. О. Хорошко, Ю. Є. Хохлачова // Сучасний захист інформації. – 2012. – № 2 (11). – С. 21–27.

46. Грищук Р. В. Адаптація положень методів теорій диференціальних ігор та диференціальних перетворень для рішення прикладних задач захисту інформації / Р. В. Грищук // Сучасний захист інформації. – 2010. – № Спецвипуск (4). – С. 13–20.

47. Грищук Р. В. Багатокритерійний синтез систем інформаційної безпеки / Р. В. Грищук, І. А. Пількевич, В. О. Хорошко та ін. // Восточно-Европейский журнал передовых технологий. – 2012. – № 5/9 (59). – С. 40–44.

Надійшла: 30.08.2012 р.

Рецензент: д.т.н., професор Петров О.С.